WIS3 – Workshop on Information Sharing & Safeguarding Standards: Summary of Workshop Discussions

December 5, 2011

On 5 December 2011, Mr. Kshemendra Paul, the Program Manager for the Information Sharing Environment (PM ISE), sponsored the Workshop on Information Sharing and Safeguarding Standards (WIS3) in Washington, DC. WIS3 built on the momentum of the 2010 standards event co-hosted with the Object Management Group (OMG) and was conducted through a series of panel discussions, presentations and break-out sessions. Attendees represented a cross-section of government (federal, state, and local), industry standards, and private sector organizations, as well as Canadian government partners. Mr. Paul noted progress in 2010 regarding standards including UML profile, NIEM advancements, data lock-down and cloud computing initiatives. Attendees were charged to be a "community of action," defining the next steps during WIS3.

Panel: *Call to Action*

Moderator: Mr. Richard Soley, Chairman & CEO, Object Management Group (OMG)

Panel:

- Mr. Kshemendra Paul, PM ISE
- Dr. Scott Bernard, Federal Chief Enterprise Architect, Office of Management and Budget (OMB)
- Ms. Kathleen Turco, Associate Administrator, Office of Government-wide Policy (OGP), General Services Administration

Topic: ***Community Building***

Panel discussion revolved around coalescing of information sharing and safeguarding standards. Working with ISE partners, PM-ISE needs to align on best practices and create a standards roadmap. Industry wants to see a viable market that is less fragmented and wants standards-based approaches to facilitate the market. A thoughtful approach through inclusion of appropriate standards in acquisition requests for information/ proposals may lead to creative and innovative ways to meet mission requirements and may assist agencies with today's shrinking budgets and allow them to move more quickly in their acquisitions. The ISE community should consider pursuing an industry-based certification and compliance approach, and leveraging acquisition power in creating an information sharing and safeguarding standards-based acquisition process. The notion of a Standards Coordinating Council supporting shared standards governance across Government, Standards Development Organizations (SDOs), and Industry Partners was introduced for consideration by the PM ISE.

In response to a question on proactive steps being taken to address privacy concerns, OMB stated that NIST Special Publication 800-53 has been updated with an Appendix J for Privacy Controls; the Federal Enterprise Architecture (FEA) 2.0 covers privacy concerns; and the Security and Privacy Profile reflects privacy concerns. Data privacy is critical to the ISE. While there are frameworks for privacy, privacy policy automation (not technology or standards) will help address data privacy concerns across organizational boundaries.

At the conclusion of this panel, the stage was set for the breakout groups, challenging each attendee to listen with standards issues in mind, make the presentations action-oriented and to look for "low-hanging fruit."

Industry-Led Breakouts: *Defining the Stack --- Federated Information Sharing Frameworks & Services*

The breakout sessions, led by industry moderators, began with presentations focused on a specific topic, and then provided an opportunity for an interactive discussion about the next generation of capabilities for information sharing across agencies. Sessions addressed the following topics:

Breakout #1 – Supporting Standardized Information Exchanges Across Government

Breakout #2 – Identity and Access Management Across Government

Breakout #3 – Federated Information Sharing Frameworks and Services

Breakout #4 – Translation of Business Requirements into Solutions

Reports from each group were presented later during the day (addressed later in this summary).

Presentation: *Department of Health and Human Services (HHS), Standards-Based Information Sharing*

Dr. Terry Cullen, Dept. of Health and Human Services (HHS), provided insight into the HHS top initiatives and lessons learned as these initiatives have been and are being addressed. Two focal points evident in these initiatives are standards and interoperability. HHS is currently developing a standard for lab results interface systems that addresses standard measures and taxonomy across providers; working to develop a standard Implementation Guide for Clinical Documents Architecture; and pursuing initiatives developed when user stories were created to bridge technical and operational requirements. Dr. Cullen addressed how lack of a common implementation of the current Immunization Data standards has hindered successful provision of correct patient care with issues resulting from varying interpretations, use of various data standard transport methods, and that raise questions of data integrity. Among the lessons learned to date are that standards must be developed and published in a timely manner to be effective --- governance is key; users of the information to be shared must adopt a standard implementation; data integrity must be managed; and always remember what the original requirements were.

A huge issue for HHS today is in working with state and local organizations on HHS initiative funding. The Affordable Care Act provides additional money to state and local organizations for many HHS initiatives; however, that funding comes in separate streams. If state and local organizations could consolidate that funding, it would provide the flexibility to deliver multi-capability solutions more efficiently and effectively.

Panel: *Standards Challenges and Solutions*

Moderator: Mr. Paul Wormeli, Executive Director Emeritus, IJIS

Panel:

- Mr. Anthony Hoang, Managing Director, NEIM PMO
- Mr. Mark E. Reichardt, President and CEO, OGC
- Mr. Scott McGrath, Chief Operating Officer, OASIS
- Mr. Dave Usery, President and CEO, URL Integration
- Dr. Richard Soley, Chairman and CEO, OMG

Topic: ***Industry Perspective on Ensuring Standards Compliance and End-User Focus Through Governance***

Discussion began with talk of the initial signing of the National Information Exchange Model (NIEM) in 2005 and the extent to which it has been adopted, i.e. across the federal government, New York, and Canada. Such broad adoption implies that NIEM remain flexible and adaptable to change and that NIEM's culture be preserved to ensure that it remains open, fluid and mission-focused; continues to be collaborative; builds on the camaraderie; uses de-centralized structures; and is non-traditional.

Great ideas from multiple stakeholders emphasize the need to better organize ideas and activities so that they can be leveraged, especially in the governance area. Education between organizations is fundamental to addressing users' urgent needs through leverage of what's been done to date. Project Springboard, a program to accredit or certify information exchanges, was discussed.

As one panel member stated, standards are not a "spectator sport" and everyone was encouraged to get on the field and play to ensure their organizational requirements are understood. Attendees, especially industry, were encouraged to use this conference to get more deeply involved in standards development, representing the practitioners (vice IT organizations), identifying profile dependencies, and standards testing.

Panel discussion concluded with lessons learned to date, including regular communication with stakeholders in forums such as WIS3 and building relationships. There is no value to having a standard that has no chance of implementation. Building pilots and performing proofs of concepts, especially relevant to the requirements, can solve real problems. It was noted that issues around policies exist; typically it is not a technical issue that hinders information sharing.

In response to an audience-posed question, panel members indicated that PM-ISE should address the human factors, rather than technical, in regards to information sharing and safeguarding standards, such as establishing a Wiki and/or an advisory council; creating and maintaining a single calendar of activities, continuing annual meetings like WIS3 and conducting frequent conference calls to discuss current activities.

In addition, the following general comments of particular note were made during this panel:

- Balance the term “best practices” with what is considered best practices for a specific organization and a specific mission at that moment.
- Establish a characterization of different standards (e.g., policy standards versus data standards, interoperability, interfaces, etc.).
- Create a feedback loop where collaboration of standards usage and implementation is managed and reported.
- Streamline NIEM process and governance.

Panel: *Love It When a Plan Comes Together*

Moderator: Ms. Amy Maida, PM-ISE

Panel:

- Breakout #1, Ms. Laura Thibodeaux, ACT-IAC
- Breakout #2, Mr. Dave Chesebrough, AFEI
- Breakout #3, Mr. Steve Ambrosini, IJIS
- Breakout #4, Mr. Larry Johnson, OMG

Topic: ***Results of Breakout Sessions***

Each breakout session chair summarized the discussions from their sessions, including plans forward. More detailed information will be available on the ISE website.

Breakout #1 – Supporting Standardized Information Exchanges Across Government

The session revolved primarily around the National Information Exchange Model (NIEM), its governance, the need for more flexibility so that it can be more readily adopted across the community and NIEM’s path forward. Mission priorities and scope as an obstacle to interagency and international collaboration were discussed as challenges within agencies and internationally for interagency/international collaboration and funding for pilots or initiatives crossing organizational boundaries. Engagement of stakeholders and continued collaboration are essential to more effective, innovative and agile approaches to interagency and international information sharing.

Breakout #2 – Identity and Access Management Across Government

The session centered on the need for a strategic vision, built on existing strategies and guidance, of where identity and access management needs to be in 5-10 years so we can ensure tactical actions are taken today that will help accomplish the end goal. Essential to the vision is defining the framework and governance over multiple aspects of sharing and safeguarding, coordinating between existing governance activities and creating governance activities where it is lacking, and providing clear guidance on adopting the vision.

Breakout #3 – Federated Information Sharing Frameworks and Services

The session identified an opportunity for a fresh start and expressed confidence that organizations could create federated capabilities across the government. Participants in this session cautioned that it will be complicated and difficult. Taking the long view, they recommended concentrating on a common mission, unifying a set of information sharing and interoperability standards, and developing a "common recipe" on how to use standards, frameworks, and architectures.

Breakout #4 – Translation of Business Requirements into Solutions

The session began with a discussion on the different language/framework tools used by defense-related agencies and civilian agencies for expressing Enterprise Architecture (EA), i.e. UPDM and MPG respectively, and how to bring them into alignment. Topics included versioning of changing formats and semantics and challenges inherent between business domains and security-classification-driven domains. The group discussed ways that PM-ISE provide leadership towards alignment.

Panel: *Town Hall, Senior Leaders Response*

Moderator: Mr. Kshemendra Paul, Program Manager, ISE

Panel:

- Mr. Al Tarasiuk, Office of the Director of National Intelligence (ODNI), Chief Information Officer
- Ms. Donna Roy, Department of Homeland Security (DHS), Information Sharing Executive
- Mr. Glenn Johnson, Department of State (DoS), Director of Messaging Systems
- Mr. Neill Tipton, Department of Defense (DoD), Director, Information Sharing & Partner Engagement OUSD(I)

Topic: ***Senior Leaders Response***

At the conclusion of the conference, senior leaders from the Government shared their thoughts. Mr. Al Tarasiuk (ODNI) said there are 17 elements within the Intelligence Community (IC) that all are connected, at some level, in a federated architecture; standards guide information sharing and exchanges across this architecture. There is a common information sharing space, but on multiple domains. Because of budget constraints, the IC is moving away from “federated” infrastructure to a “common” infrastructure. A new vision for a common IC architecture includes Cloud Computing, Single Common Workstation configuration, and “Smart Data” protected through identity and access management.

According to Ms. Donna Roy (DHS), the information sharing challenge is finding a way to provide identity information based on policy. Standards will help the community automate trust and change the culture. The goal should be to provide data in near real time and in an ingestible format. Any framework that is developed must include capabilities to audit and measure data. The community should drive toward “data independence” - data that is smart enough to know it is secure, auditable, mobile, and agile.

Mr. Glenn Johnson (DoS) stated that information sharing is a priority at the State Department, as information must be shared with embassies all over the world. He cited lessons learned from the provision of metadata tagging tools that were not accepted by the user community, specifically calling out that ownership is key, i.e. users must “own” the tools. He also stated that role-based access controls with record management policies are critical.

Mr. Neill Tipton (DoD) shared lessons learned with information sharing initiatives focused on Afghanistan, stating that they were deployed too slowly and the end capability did not meet expectations. Converging standards will help implementation and shorten development time. Mr. Tipton stated that the Defense Intelligence Information Environment (DI2E), which is fundamentally focused on standards, will provide a DI2E storefront for DoD, IC and other communities to share services and service components. Rather than thinking “who can I share this information with” after arriving at a technical solution, the policy should be flipped, i.e. think about “if I want to share information” before arriving at a technical solution. Technology solutions for the latter provide for multiple partners for future information sharing.

In closing, the following statements were made:

- ODNI: Governance is key for anything standards related. We need to agree on the governance structure and then move forward.
- NIEM PMO: Agility and simplicity in architecting standards is key.
- DoS: Give users tools that they are motivated to use.
- DoD: Governance is critical, but can’t be top-down and needs to include humanitarian or the coalition forces stakeholder perspective.

The PM, ISE ended the WIS3, stating “We intended to build a Community of Action here today, and I think we did that.” The PM ISE will continue working with the community on the next steps and near- and long-term actions identified at the WIS3.